UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,239	01/26/2001	Jeffrey Bruce Lotspiech	ARC920010006US1	6974

7590 08/17/2004

John L. Rogitz
Rogitz & Associates
Suite 3120
750 B Street
San Diego, CA 92101

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/771,239	LOTSPIECH ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *see Office Action*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are pending in the present application. The Information Disclosure Statements received 26 January 2001, 15 February 2001, and 16 September 2002 have been considered.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 2-3, 13-14, and 22-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 2, 13, and 22 recite the limitations "determining whether the traitor subset represents at least one traitor receiver" and dividing the subset based on that determination. However, Claims 1, 12, and 21, from which the claims respectively depend, state that a traitor subset is identified "as containing at least one leaf representing a traitor receiver". It appears that these two limitations perform the same step. Therefore, it is unclear whether the limitation of the dependent claims refers to a second determination or is performing the same step as in the independent claims, which renders the claims indefinite. For purposes of applying the prior art, it has been

assumed that the limitation of the dependent claims refers to the same step as in the independent claims.

Claims 3, 14, and 23 are rejected due to their dependence on a rejected claim.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3 are rejected under 35 U.S.C. 102(e) as being anticipated by Schwenk, US Patent 6222923.

In reference to Claim 1, Schwenk discloses a method including receiving a set of subsets derived from a tree including leaves, each of which represents a receiver (column 3, lines 24-33); identifying a traitor subset as containing at least one traitor receiver (column 4, lines 9-13); and identifying and disabling the traitor receiver (column 4, lines 33-36).

In reference to Claims 2 and 3, Schwenk further discloses dividing the traitor subset into child subsets and removing complementary subsets (column 4, lines 8-33).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 4-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Yoshida et al, "A Subscriber-Excluding and Traitor-Tracing Broadcast Distribution System".

In reference to Claims 4, 29, and 30, Schwenk discloses everything as applied to Claim 1 above. However, Schwenk does not explicitly disclose encoding subsets with a false key. Schwenk also does not disclose traitor receivers embodied in a clone.

Yoshida discloses a method and system for excluding and tracing traitor subscribers to a broadcast distribution system. In reference to Claims 4 and 30, Yoshida discloses that the method includes encoding subsets with a false key (the special value of page 249, column 2, lines 15-26). In reference to Claim 29, Yoshida discloses using a captured or cloned pirate decoder to identify a traitor (page 249, column 2, lines 32-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schwenk to include encoding subsets with a false key and to further include the use of a clone, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claims 5-7, Yoshida further discloses executing a binary search (page 254, column 1, lines 19-25).

In reference to Claim 8, Schwenk discloses everything as applied to Claim 1 above. Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). However, Schwenk does not explicitly disclose encrypting the false key with the subset keys.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encrypting a false key (page 249, column 2, lines 15-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schwenk to include encrypting the false key with the subset key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claims 9 and 10, Schwenk further discloses that each receiver is assigned keys from nodes above the receiver in the tree (column 3, lines 42-58).

In reference to Claim 11, Schwenk further discloses initializing a spanning tree (column 4, lines 8-33).

In reference to Claim 12, Schwenk discloses a computer program device including a means for accessing a tree (column 3, lines 24-33), encrypting a session key (column 3, lines 55-58), identifying a traitor subset (column 4, lines 9-13), and using the traitor subset to identify and disable the traitor device (column 4, lines 33-36). However, Schwenk does not explicitly disclose encrypting a false key.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encrypting a false key (page 249, column 2, lines 15-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schwenk to include encrypting the false key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claims 13 and 14, Schwenk further discloses dividing the traitor subset into child subsets and removing complementary subsets (column 4, lines 8-33).

In reference to Claims 15-17, Yoshida further discloses executing a binary search (page 254, column 1, lines 19-25).

In reference to Claim 18, Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). Additionally, Yoshida further discloses encrypting a false key (page 249, column 2, lines 15-26).

In reference to Claim 19, Schwenk further discloses that each receiver is assigned keys from nodes above the receiver in the tree (column 3, lines 42-58).

In reference to Claim 20, Schwenk discloses a system for determining the identity of a traitor receiver and rendering it useless for decrypting data (column 4, lines 33-36). However, Schwenk does not explicitly disclose using a false key to encode subsets.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encoding subsets with a false key (page 249, column 2, lines 15-26). Yoshida further discloses using the captured pirate receiver for identifying and disabling the traitor receivers (page 249, column 2, lines 32-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Schwenk to include encoding subsets with a false key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claim 21, Schwenk further discloses receiving a set of subsets derived from a tree including leaves, each of which represents a receiver (column 3, lines 24-33); identifying a traitor subset as containing at least one traitor receiver (column 4, lines 9-13); and identifying the traitor receiver (column 4, lines 33-36).

In reference to Claims 22 and 23, Schwenk further discloses dividing the traitor subset into child subsets and removing complementary subsets (column 4, lines 8-33).

In reference to Claim 24, Yoshida further discloses encoding subsets with the false key (page 249, column 2, lines 15-26).

In reference to Claim 25-27, Yoshida further discloses executing a binary search (page 254, column 1, lines 19-25).

In reference to Claim 28, Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). Schwenk additionally discloses that each receiver is assigned keys from nodes above the receiver in the tree (column 3, lines 42-58). Additionally, Yoshida further discloses encrypting a false key (page 249, column 2, lines 15-26).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Davida, US Patent 4417338, discloses a system and method for sharing a key among multiple receivers in which, if more than a certain number of receivers are compromised, then the key cannot be recovered and thus the receivers are disabled.

b. Naito, US Patent 5125028, discloses a television scrambling system that includes the use of a false key to foil pirates.

c. Iwasaki, US Patent 6651149, discloses a storage medium that protects against illegal copying of data stored in the medium by detecting whether false keys or certificates have been used.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (703) 305-8902. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (703) 306-3036. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100